самонавчання за допомогою єдиної методичної бази, мультимедійних підручників та електронної бібліотеки на обчислювальному центрі навчального закладу, перевірки знань з використанням проміжного та підсумкового тестувань як викладачем так і за допомогою тестуючих програм на ПЕОМ.

Анна Влас
Маріупольський державний університет
Маріуполь, Україна

АПАРАТНО-ПРОГРАМНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

У статті йдеться про апаратно-програмні засоби ідентифікації користувачів при доступі до комп'ютерної інформації. Розглядаються методики ідентифікації та приклади програм, за допомогою яких реалізуються наведені напрями досліджень.

Ключові слова: засоби захисту інформації, користувач, ідентифікація, аутентифікація, дактилоскопічне дослідження, фонографічний метод.

В статье говорится о аппаратно-программных средствах идентификации пользователей при доступе к компьютерной информации. Рассматриваются методики идентификации и примеры программ, с помощью которых реализуются указанные направления исследований.

Ключевые слова: средства защиты информации, пользователь, идентификация, аутентификация, дактилоскопические исследования, фонографический метод.

The article deals with hardware and software for user identification when accessing computer information. We consider methods of identification and sample programs, through which are implemented research areas.

Keywords: data protection, user, identification, authentication, fingerprint research phonographic method.

Останнім часом, у зв'язку зі збільшенням загроз для комп'ютерної інформації, все більше уваги приділяється завданням удосконалення існуючих та розробці нових засобів захисту інформації в комп'ютерних системах від небажаного доступу з боку неавторизованих користувачів.

Відповідно до Закону України «Про інформацію», захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї [2].

На сьогодні існують три основні підходи, що забезпечують надійний захист даних та ідентифікацію користувачів: парольний; апаратний (електронний) та біометричний.

Поступово все більшого поширення одержує багатофакторна ідентифікація, коли для визначення особистості користувача застосовується відразу кілька параметрів. Це так звані апаратно-програмні засоби. Вони реалізують ті ж функції, що апаратні і програмні засоби окремо (перешкоджання фізичного проникнення до інформації; шифрування інформації, видалення залишкової, тестового контролю системи захисту), а також мають власні проміжні властивості.

Щоб отримати доступ до системи, користувач повинен пройти два етапи. Перший – ідентифікація, при якій визначаються ті його характеристики, яких не мають інші користувачі, другий – аутентифікація, при якій відбувається порівняння визначеного в ході першого етапу користувача з загальним зареєстрованим списком користувачів, які мають право доступу до системи. Однак, саме перший етап дозволяє розробникам систем захисту інформації впровадити винайдені апаратно-програмні комплекси [3, 157].

Однією з найбільш простих і ефективних в реалізації методик є проведення дактилоскопічного дослідження. У дактилоскопічних пристроях використані високі технології ідентифікації особистості, поєднані з функціональністю і ергономічністю сканерів – пристроїв, за допомогою яких відбувається так зване безфарбне дактилоскопіювання особи. Принцип дії сканерів полягає в тому, що світло, відбите з поверхні відбитка пальця, проходить через призму і потрапляє на спеціальний сенсор, який фіксує чітке зображення папілярного візерунка. Це висококонтрастне зображення, що містить інформацію про глибину і структуру малюнка, проходить процес оцифрування. Доступ буде заборонений будь-якому користувачеві, чий відбиток пальця не співпаде із зареєстрованим [1, 5].

Більш складною в реалізації є методика ідентифікації за структурою і взаєморозташування кровоносних судин руки, яка індивідуальна у кожної людини. Це продукти фірм «BK SYSTEMS Co. Ltd-BK-300S», фірми «Ethentica-Ethenticator MS3000» – сенсорна система перевірки, що включає AuthenTec – апарат, що пропускає через кінчик пальця користувача електричний струм дуже малої потужності, що створює тим самим карту тканин з декількох рівнів, яка дозволяє провести ідентифікацію навіть у тих випадках, коли фаланги пальців пошкоджені. Особливістю цих пристроїв є те, що в процесі їх роботи відбувається дослідження внутрішніх органів людини – структури кровоносних судин руки, їх взаєморозташування, розміри, а не поверхні пальця.

На апаратно-програмному рівні реалізується й фонографічний метод ідентифікації. Його мета – встановлення особи за спектральними характеристиками голосу, які є суто індивідуальними для кожної людини. Реалізація даного методу пропонується в продукті компанії «Vertiel-VoiceCheck», що дозволяє ідентифікувати користувача за допомогою зіставлення виголошеної ним конкретної фрази із зразками, наявними в системі.

Ще одним напрямком є комплекси, засновані на портретній ідентифікації – зіставленні, суміщенні, накладанні. З невпинним розвитком обчислювальної техніки новий імпульс вдосконалення отримали методи, що дозволяють ввести в процес дослідження кількісні характеристики – ідентифікація особистості, на підставі сукупності кутових вимірювань між найбільш представницькими точками. Однією з найуспішних форм реалізацій зазначеного методу ідентифікації є комплексна система «One-on-one Facial Recognition». Даний комплекс, використовуючи відео- та цифрові камери, розпізнає особу і забезпечує так званий «ненав'язливий» контроль над користувачем інформаційної системи та паралельно контролює доступ в будівлю або приміщення, де вона розташована. При першій інсталяції комплексу користувач повинен зареєструвати своє обличчя в базі даних. У результаті цієї процедури система «One-on-One» створить цифровий підпис, пов'язаний із зображенням конкретної особи. При подальшому використанні комплексу, система буде ідентифікувати зображення особи користувача зі збереженою в базі.

Створюються пристрої, що дозволяють ідентифікувати особу за якою-небудь однією ознакою. Так, пристрій EyeDentify's ICAM 2001 використовує камеру з сенсорами, які з короткої відстані (менше 3 см) вимірюють властивості сітківки ока. Людині достатньо поглянути одним оком в отвір камери ICAM 2001 і система ухвалює рішення про право доступу.

Найбільш складним у реалізації є продукт, який базується на ідентифікації почерку, зокрема за підписом. Приклад тому – eSign – програма що використовує спеціальну цифрову ручку і електронний блокнот для реєстрації підпису. У процесі реєстрації eSign запам'ятовує не тільки саме зображення підпису, але й динаміку руху пера.

Розвиваються комплекси, засновані на псіфізіологіческіх особливостях роботи за комп'ютером конкретної людини. Це, перш за все, так звана ідентифікація користувача за допомогою його клавіатурного почерку – пакет ESL фірми «Electronic Signature Lock». Він заснований на тому, що робота на клавіатурі є послідовне натискання і відпускання певної сукупності клавіш. При закладі текстової інформації, як правило, здійснюється послідовне включення і виключення окремих клавіш клавіатури, що спрощує процес фіксації і обробки часових параметрів клавіатурного почерку.

Це лише частина з тих систем захисту інформації, які використовують для ідентифікації особи біометричні характеристики конкретної людини з метою профілактики вчинення ним несанкціонованого доступу.

Зазначені апаратно-програмні комплекси і системи в даний час є на ринку інформаційних товарів і послуг та доступні майже кожній людині. Наявність такого роду комплексів, істотно підвищує рівень захисту практично будь-якої інформаційної системи дозволяє не тільки своєчасно встановити факт несанкціонованого доступу, але й запобігти його вчиненню.

Розглянувши існуючі засоби ідентифікації користувачів, можна впевнено зробити висновок, що надалі у міру зростання обчислювальних потужностей все більш запитаним буде вживання систем багатофакторної ідентифікації, що дозволить значно підвищити рівень надійності захисту інформації в системі.

Література:

1. Голубів, Г. А. Сучасний стан та перспективи розвитку біометричних технологій / Г. А. Голубів, Б. А. Габриелян // Нейрокомп'ютери: розробка, застосування. 2004, №10.
2. Закон України «Про інформацію» від 02.10.1992 № 2657-XII
3. Щелов, А. Ю. Захист комп'ютерної інформації від несанкціонованого доступу / А. Ю. Щеглов. – СПб.: Політехніка, 2001. – 240 с.

Ірина Московкіна
Донецький національний університет
Вінниця, Україна

ІНФОРМАЦІЙНА ПІДТРИМКА ДОКУМЕНТООБІГУ СІЛЬСЬКОЇ РАДИ

Розглянуто правові засади регулювання та перспективи розвитку інформаційного забезпечення органів державного управління та місцевого самоврядування, проаналізовано документообіг Стрижавської сільської ради, розроблено рекомендації щодо інформаційної підтримки органу місцевого самоврядування.

Ключові слова: місцеве самоврядування, інформаційна підтримка, електронний документообіг, продукти корпорації Microsoft

Рассмотрены правовые основы регулирования и перспективы развития информационного обеспечения органов государственного управления и местного самоуправления, проанализирован документооборот Стрижавского сельского Совета, разработаны рекомендации по информационной поддержке органа местного самоуправления.

Ключевые слова: местное самоуправление, ИНФОРМАЦИОННая поддержка, электронный документооборот, продукти корпорации Microsoft

Legal frameworks of adjusting and prospect of development of the informative providing of organs of state administration and local self-government are considered, circulation of documents is analysed Strigavskoj village Soviet, worked out to recommendation on informative support of organ of local self-government.

Tags:Local self-government, informative support, electronic circulation of documents, corporation Microsoft

Процес організації роботи з документами та його інформаційне